An IT Director’s Guide to Communicating Security Needs to the Executive Team

[ Giving Security the Attention It Deserves ]

Pratum
INTRODUCTION

Information security is slowly gaining the respect it deserves, but there are many obstacles still getting in the way. One of the biggest hurdles that IT Directors and Information Security Officers (ISO) face is the communication of security concerns with their executive team. Information technology professionals innately understand the threats posed by cybercriminals, but the business decision makers may have a ways to go.

This paper discusses effective ways to communicate security concerns and solutions to the executive team – providing talking points and suggestions. There are three topics that are bound to pique the interest of the C-suite: Protecting Business Reputation and Brand Image, Preventing an Expensive Security Breach, and Vendor & Client Requirements. The more prepared you are with these topics, the better chance you have at earning the trust of the decision makers.

Executive Insights

Business executives are busy.
Executives expect concise analysis and well-thought solutions. Prepare reports and presentations to focus on the key business issues, challenges, and recommended actions for moving projects forward.

Business executives make decisions based on risk.
Be prepared to discuss the business impact of the security problem and your proposed solution, and be ready to talk dollars.

Business executives don’t often love dealing with security.
This is not ideal, but it should come as no surprise - there are few of us who are passionate about security. However, if you are able to communicate the importance of security to your business, you will have the advantage.
PROTECTING BUSINESS REPUTATION AND BRAND IMAGE

This topic will be of interest to Marketing, Sales, and the CEO. There are few things more important to these departments than the reputation of the business and how it is perceived by clients and prospects.

The significance of perception.

There are many factors that go into building and maintaining a brand; everything from an organization's mission and vision to its marketing, product quality, and customer experience. An organization is defined by how people perceive and interact with its brand. This is what drives the purchase decision.

Organizations spend a lot of time creating new products and service offerings to compete in the market space. Within the organization, information security needs will compete for resources, and cyber criminals can take advantage of this condition. Ironically, security breaches can have a much larger impact on the perception of an organization than any piece of marketing or sales communication.

As presented in the 2016 Cost of Data Breach Study: Global Analysis by The Ponemon Institute, US organizations pay the highest cost for losing customers after a data breach. On average, the cost of lost business was $3,970,000. This cost component includes the abnormal turnover of customers, increased customer acquisition activities, reputation losses and diminished goodwill.

The US also has the highest percentage of indirect costs associated with a data breach at 66% of total cost. This is an astonishing number, which includes the time, effort and other organizational resources spent during the data breach resolution. It also includes the loss of goodwill and customer churn.

On average, the cost of lost business due to a data breach was

$3,970,000

1. Forrester: Planning For Failure, 2015 - https://www.forrester.com/Planning+For+Failure/fulltext/-/E-res60564
PREVENTING AN EXPENSIVE SECURITY BREACH

There are numerous costs associated with data loss, including but not limited to fees associated with consulting, attorneys, digital forensics, and insurance. Data breaches can be a lot of things, but inexpensive isn’t one of them. If this topic doesn’t get the attention of your CFO, nothing probably will.

As an IT director or manager, it is your responsibility to present security risks to the executive team. This must be done in a manner that can be fully understood and appreciated by executives. What is the easiest way to communicate? Talk numbers. If there is uncertainty about the potential impact to your business, execs will be reluctant to approve any action. Discuss the financial risk and potential impact of a security breach, and you will garner their attention.

The threat is real.

Security awareness is on the rise, but many people still don’t believe a security incident will happen to them or their company. To many, it is easier to stand by and hope for protection than it is to do something about it. However, the lack of preparation will eventually catch up to those who sit and do nothing, and when it does, it will be more painful and costly than the proactive approach.

At least 60% of enterprises will discover a breach of sensitive data in the next year. (Forrester 2015)

VENDOR & CLIENT REQUIREMENTS

As security awareness rises, so do expectations of vendors and clients. Organizations have begun including information security as a major emphasis in their due diligence process. Vendors and clients are actively searching for partners that value security and make it a top priority.

It is not uncommon for companies to lose out on business due to their lack of security controls. Many organizations won’t do business with a company that hasn’t received SOC 2 Compliance Reporting (service organizations) or gained compliance with HIPAA (healthcare), PCI (payment card), or FISMA (Federal contracts) requirements. Security is too important to ignore. Take-charge of your security, and your business will benefit.

“We won’t even consider a vendor if they haven’t performed a SOC 2.”

-- anonymous exec
Financial Institution
When talking with executives, be organized. This doesn't mean that you have to deliver a PowerPoint presentation every time you conduct a meeting, but you should have your plan in order. You will be expected to answer some pointed questions, and you may only get one shot.

**Start with a conversation.**

Start by asking some of your own questions. Establish a two-way conversation, and clearly explain the situation. This approach will give insight into the perspectives of the executives. Use this as an opportunity to learn from them and to build your case.

Questions you can ask to get a conversation started:

- How would you describe our brand and what it means to our customers/clients?
- What have we done, and continue to do, to build our reputation?
- What are our plans for our brand in the future?
- Do you have any concerns with our business’ security risks? If so, what are they?
- Has our executive team discussed a strategic security plan?
- Have we lost any prospective business due to a lack of security controls?

The above questions get executives thinking about everything they have done to help build and grow the company. There is much pride in that effort, which you can leverage when communicating the ways that security, or lack thereof, will directly impact their efforts.

Take advantage of the opportunity to meet with executives, and be prepared to support your analysis and recommendations. If you do not already understand the executives’ approach to business, then take some time to learn their perspectives. After all, they will make the decision on whether or not you get the funding you need.
Move forward with the hard truth.
Executives have enough to worry about; throwing a data breach into the mix will make their jobs even more difficult. Take this time to talk with them about current and prospective customers. It is important to discuss both short-term and long-term impacts of a security breach.

If you need help explaining to executives the impact a security incident can have on clients and prospects, please use the following examples to support your case. Below is a section of information that will be helpful to all industries. There are also discussion suggestions specific to manufacturing, retail, healthcare, technology, and banking & finance. If you are in one of these industries, review the respective sections for specific talking points.

### All Industries

**Client Impact**
Our clients will be concerned if they hear we have experienced a security breach. Regaining their trust can be slow, and a drop-off in sales can be expected while rebuilding that trust.

**Prospective Client Impact**
All else equal, a prospective client will select an organization that hasn't experienced a security breach. Why would they willingly put themselves at risk with a company that has a proven record of losing sensitive information?

### Manufacturing

**Client Impact**
Intellectual property is one of the most valued assets of our manufacturing clients. If we were to lose their sensitive information, it would drastically impact our relationship. There are contractual obligations, legal ramifications, and reputation issues when dealing with security.

**Prospective Client Impact**
A security breach would impact our reputation with prospective clients. If our company is perceived as careless and negligent, it would likely remove us from consideration for many future projects.

### Retail

**Client Impact**
How would our retail customers respond if their credit card information was stolen from our stores? A survey from CNBC reveals that 15 percent of consumers generally stopped shopping at breached retailers and 23 percent generally stopped using breached payment methods. If customers move from credit card payment to cash payment, their average ticket size decreases between 10 and 20 percent.

**Prospective Client Impact**
Shoppers don't soon forget security breaches. Nearly a full year after Target's security breach, customers indicated that their fears of the breach's impact would still affect their spending plans during the holiday season.

---

**Healthcare**

**Client Impact**

HIPAA impacts nearly everything we do, but complying with the regulations doesn’t make us secure. A security breach could publicly expose patient information, resulting in fines and patient backlash. As a healthcare provider we are required to report security breaches and inform victims. The breach will become known, and the impact will be significant.

**Prospective Client Impact**

HIPAA fines are one thing, but losing prospective patients to competing hospitals and clinics can be devastating. People are often very private when it comes to their healthcare information, and they do not respond well to losing that confidentiality.

**Technology**

**Client Impact**

Technology can be a very tricky industry. Changes in innovation occur at rapid speeds, and customer options grow by the week. There is always the threat of a new company overtaking our market share. If our clients’ account information is stolen, or they are locked out of their system due to a security breach, they may quickly look elsewhere for a new technology partner.

**Prospective Client Impact**

There are often numerous options when it comes to technology solutions. If our company’s reputation is tarnished by a security breach, it will be difficult to convince businesses that our technology solutions are securely built. If we can’t convince anyone of that, then our business will be in trouble.

**Banking & Finance**

**Client Impact**

Competition is fierce in the banking and financial industry. We have competitors on every corner and online. Our reputation is everything. If our customers begin to think that we can’t protect their assets, they will leave in droves.

**Prospective Client Impact**

Over the past decade, the reputation of banks has taken a major hit. We must do everything in our power to rebuild and maintain trust of our communities. It starts with securing our customers’ information and assets.
Now, propose the solution.

Executives are going to look to you for suggestions and security knowledge. Here's the key: use what you've learned from conversations with executives to help you in preparing your case. Take your time with this process; be thorough. You may already know your security risks, or at least some of them. Now, you must discover options for the solution.

You may need to talk with a security consultant or advisor before understanding which solution is appropriate for your risk(s). The best vendors will listen to your risks and guide you toward the appropriate solutions. Once you have an understanding of your needs and narrow down your vendor options, begin requesting estimates.

Compile the most compelling estimates, and present them to your executives. Prior to your meeting, be sure to establish a timeline/schedule for the work. Without a timeline, the project is bound to get derailed.

**Presenting to Executives**

Here are the four must-haves when presenting to executives.

### The Problem (Security Risk)

This is where you discuss the security risks and how they could impact your business. Use numbers to explain the potential loss in revenue, regulatory fines, legal fees, etc., if the risk becomes reality. Executives need to know how the risk could negatively affect the company and the likelihood of the risk becoming a security incident.

### The Solution

Let the executives know that you have a solution to the problem. There is a way to reduce/mitigate risk, and you know how to do it. Explain in basic business terms how the solution will solve the issues at hand. Don’t get overly technical, but make sure they understand how the solution will improve the situation.

### The Cost

Talk with vendors to get your estimates, then present the estimate with the best value (not necessarily the least expensive) to the executives. The cost of implementing a solution should be less than the cost that could be incurred if the solution were not implemented. If your solution costs more than the security risk could actually cost the organization, no one will buy into it.

### The Timeline

Work with your vendor and your team to understand how long this process will take. Give yourself a little bit of freedom for schedule adjustments, but do your best to make it accurate.